REMARKS

By this paper, claims 9-10, 13, 15-20, 23 & 25-28 have been amended, claims 14 and 24 have been cancelled and new claim 29-32 has been added, such that claims 9-13, 15-23 and 25-29 remain pending, of which claims 9 and 19 are the independent claims at issue. Support for the claim amendments and new claims is found throughout the specification, including, but not limited to the disclosure found within paragraphs [0046]-[0065] and Figure 3.

In the Final Office Action, mailed March 14, 2008, claims 9-28 were rejected under 35 U.S.C. 102(b) as being anticipated by Anderson et al. ("Protected EAP Protocol (PEAP")) hereinafter Anderson. However, Applicant respectfully submits that Anderson fails to anticipate or render the claimed invention obvious.

As recited in the claim listing above, the pending claims are generally directed to embodiments in which a client authenticates with a server through various request and response communications. These communications include a first request sent from a server to a client and that includes authentication mechanisms deployed at the server and a server nonce. A corresponding first response is sent from the client to the server and includes a client public key, a client nonce and a selected set of the authentication mechanisms that were included in the first indication of the authentication mechanisms received from the server and that are also deployed at the client computing system. A tunnel key is then derived for encrypting content transferred between the client and the server. The tunnel key comprises a hash of a concatenation of the client public key together with the server nonce and the client nonce. A second server request is then sent to the client with authentication content that is encrypted with the tunnel key and that includes a server challenge, a mutually deployed authentication method and a trust anchor. The client decrypts the authentication content with the tunnel key to reveal the mutually deployed authentication mechanism, the server challenge and the trust anchor. The client then sends a second response to the second server request and that includes response data that is responsive to the unencrypted authentication content, including at least one of a client challenge, a hashed message authentication code that corresponds to the server challenge, or a client authentication signature, and that is used for authenticating the client computing system with the server computing system according to the mutually deployed authentication mechanism.

Notably, claim 9 recites a method for participating in authenticated communications, as described above, which is recited from the perspective of the client. Claim 19, on the other hand, recites a similar method from the perspective of the server.

In rejecting the claims, it was asserted that Anderson discloses a first response that includes at least a second indication of the authentication mechanisms deployed at both the client computing system and the authentication mechanisms deployed at the server computing system (OA page 3). Applicants respectfully disagree. Instead, it is noted that Anderson discloses that "[t]the client_hello message contains the client's TLS version number, a sessionID, a random number, and a set of TLS ciphersuites supported by the client." (p. 7, 4th full paragraph). A corresponding "server_hello handshake message contains a TLS version number, another random number, a session Id, and a TLS ciphersuite." (p. 8, 2nd full paragraph). Notably, the TLS ciphersuite included in the server_hello message is a TLS ciphersuite chosen from those offered by the client. ("The server will also choose a TLS ciphersuite from those offered by the client.") (p. 8, 3rd full paragraph). Accordingly, Anderson discloses that the client identifies a plurality of ciphersuites from which the server selects one of the ciphersuites to include in a message to the client. Anderson does not, however, teach or suggest that a client first receives a server request that includes a first set of authentication mechanisms (or ciphersuites) deployed by the server and then responds with a communication that includes a set of authentication mechanisms (or ciphersuites) that are selected from the first set of authentication mechanisms identified by the server and that are also deployed by the client.

Anderson also does not appear to disclose that a tunnel key is used to encrypt content transferred between the client and server (including subsequent authentication information that includes a server challenge, a mutually deployed authentication method and a trust anchor) as claimed, and particularly when the tunnel key comprises a concatenation of the client public key together with server and client nonces communicated in the initial request and response.

In rejecting claim 14, which is now cancelled, but which clarified one embodiment of the tunnel key, the Examiner asserted that Anderson discloses TLS and hence the negotiation of a key. However, it is noted that claim 14 did not require the *negotiation* of a tunnel key. Accordingly, it is unclear whether the Examiner was instead referring to the negotiation of authentication methods. It is also noted that even if Anderson did disclose TLS, this does not

presumptively teach or suggest that a tunnel key comprises a concatenation of the client public key together with server and client nonces, as claimed. In rejecting claim 14, the Examiner refers to page 15. However, it is noted that page 15 discloses many different types of master keys, but none of them are described in the recited disclosure as comprising a concatenation of the client public key together with server and client nonces that are communicated in the initial request and response, as claimed, and particularly as recited in combination with the other recited claims, such as being used to encrypt a server challenge, a mutually deployed authentication method and a trust anchor.

Anderson also fails to disclose or suggest any embodiment, such as described above, and which also includes a client using the tunnel key to decrypt the server challenge, the mutually deployed authentication method and the trust anchor and to thereafter send the server a second response that includes at least one of a client challenge, a hashed message authentication code that corresponds to the server challenge, or a client authentication signature, and which is used for authenticating the client computing system with the server computing system according to the mutually deployed authentication mechanism. (see claims 30-32).

Anderson also fails to disclose or suggest any embodiment, as described above, and which further includes the use of a first response that includes a plurality of security associations (in addition to the plurality of authentication mechanisms) and particularly wherein the second request includes one of the plurality of security associations selected from the plurality of security associations, as recited in claim 29.

In view of the foregoing, Applicant respectfully submits that the foregoing embodiments, including those recited in independent claims 9 and 19 are distinguished from the cited art of record and such that all of the rejections to the corresponding dependent claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the dependent claims.[1]

[1] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

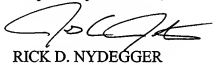
In fact, it will be noted that many of the dependent claims even further distinguish the claimed invention from the cited art, including the embodiment which requires that the client provide a plurality of public keys within the first response to the server's first request and as recited in claims 13 and 23, for example.

For at least the foregoing reasons, Applicant respectfully submits that the pending claims are distinguished over the cited art and are in condition for allowance.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at 801-533-9800.

Dated this 14th day of July, 2008.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant
Customer No. 47973

JCJ:ahy:laf
1605674_1